A REPORT
TO THE
MONTANA
LEGISLATURE

INFORMATION SYSTEMS AUDIT

Statewide Disaster Recovery Planning for Information Technology Systems

Department of Administration

FEBRUARY 2010

LEGISLATIVE AUDIT
DIVISION

10DP-01

Information Systems Audits

Information Systems (IS) audits conducted by the Legislative Audit Division are designed to assess controls in an IS environment. IS controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed. We conducted this IS audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our finding and conclusions based on our audit objectives.

Members of the IS audit staff hold degrees in disciplines appropriate to the audit process. Areas of expertise include business, accounting, education, computer science, mathematics, political science, and public administration.

IS audits are performed as stand-alone audits of IS controls or in conjunction with financial-compliance and/or performance audits conducted by the office. These audits are done under the oversight of the Legislative Audit Committee which is a bicameral and bipartisan standing committee of the Montana Legislature. The committee consists of six members of the Senate and six members of the House of Representatives.

Direct comments or inquiries to:
Legislative Audit Division
Room 160, State Capitol
P.O. Box 201705
Helena, MT 59620-1705
(406) 444-3122

Reports can be found in electronic format at:
http://leg.mt.gov/audit

LEGISLATIVE AUDIT DIVISION

Tori Hunthausen, Legislative Auditor
Monica Huyg, Legal Counsel

Deputy Legislative Auditors
James Gillett
Angie Grove

February 2010

The Legislative Audit Committee
of the Montana State Legislature:

We conducted a statewide Information Systems audit of the development of disaster recovery (DR) planning for information technology (IT) systems. The overall purpose was to determine the status of IT DR in state government.

Overall, we found state agencies are aware of the need for DR planning for IT systems and most have incorporated some elements of a DR plan. However, we found the level of understanding of DR planning varies between agencies and some are more prepared to deal with extended system outages than others. We believe the inconsistency can be resolved by establishing centralized policy and corresponding guidelines requiring complete and consistent DR plans for critical IT systems.

We wish to express our appreciation to Montana's agencies and universities for their cooperation and assistance.

Respectfully submitted,

/s/ Tori Hunthausen

Tori Hunthausen, CPA
Legislative Auditor

Room 160 • State Capitol Building • PO Box 201705 • Helena, MT • 59620-1705
Phone (406) 444-3122 • FAX (406) 444-9784 • E-Mail lad@mt.gov

TABLE OF CONTENTS

Figures and Tables

Figures

Appointed and Administrative Officials

Department of Administration

Janet R. Kelly, Director

Sheryl Olson, Deputy Director

Dick Clark, State Chief Information Officer

Dawn Pizzini, Security and Continuity Services Officer

REPORT SUMMARY

Disaster Recovery Planning for IT Systems

Business continuity is a series of processes implemented by an organization to ensure the continued availability of services and resources. An important element of business continuity is disaster recovery (DR) planning for information technology (IT) systems. DR planning is a set of steps, communications, and responsibilities that are to be executed in the event of an interruption of services. An effective DR plan is documented and designed to quickly and completely reestablish a system or service following a service interruption or disaster resulting in minimum loss to the organization. We performed audit work to determine the current status of DR planning throughout state government.

Within Montana state government, many business processes are reliant on computer systems, with over $120 million in IT expenditures annually. Recently, the Information Technology Services Division (ITSD) at the Department of Administration has inventoried 427 computer systems in service throughout state government, each providing varied levels of support for agency business operations. If agencies are not developing DR plans to minimize system disruptions, the result could be extended unavailability of government services critical to the safety and welfare of the general public, as well as the day to day operations of state government.

To determine the status of DR planning throughout state government, we reviewed the level of planning done for critical systems at multiple agencies, comparing elements in place with established criteria for complete DR planning. Based on our work, we conclude state agencies are aware of the need for DR planning for IT systems and most have incorporated some elements of a DR plan. However, we found the level of understanding of DR planning varies between agencies and some are more prepared to deal with extended system outages than others. We believe the inconsistency can be resolved by establishing centralized policy and corresponding guidelines requiring complete and consistent DR planning for IT systems.

Chapter I – Introduction and Background

Introduction

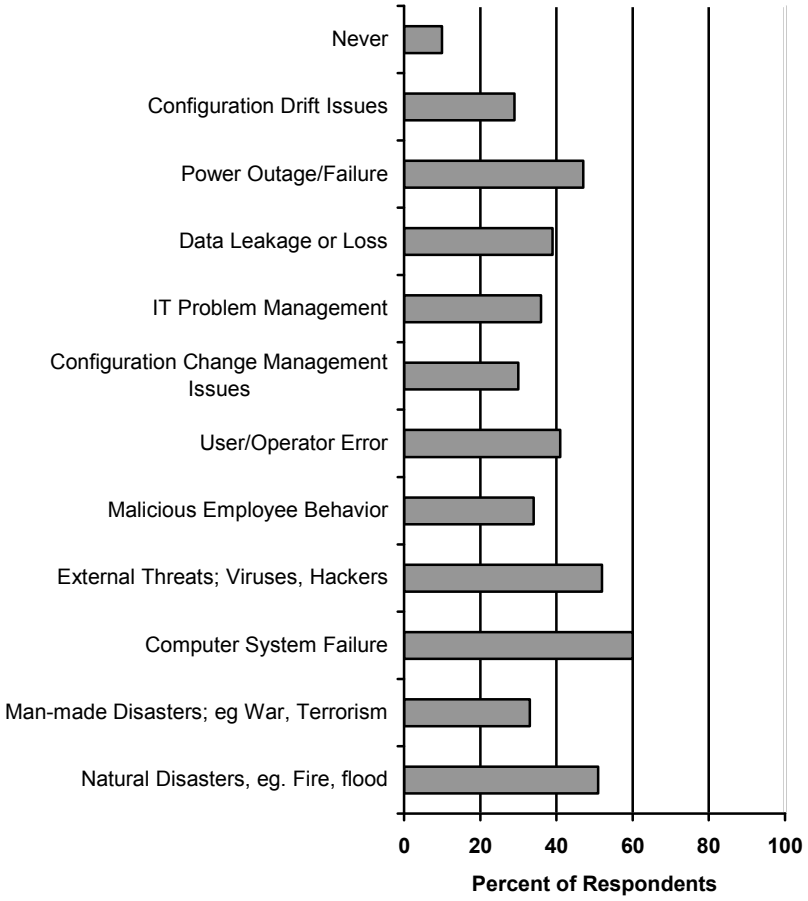
Business continuity (BC) is a series of processes implemented by an organization to ensure the continued availability of services and resources. BC planning include identification of critical services, development of continuity of operations procedures, duplication and storage of documents and data, identification of key staff, and identification of order of succession. A number of state agencies have implemented these elements. In addition, the Information and Technology Services Division (ITSD) at the Department of Administration includes the Office of Security and Continuity Services to provide centralized guidance on BC. Another important element of business continuity is disaster recovery (DR) planning for information technology (IT) systems. DR planning is a set of steps, communications, and responsibilities that are to be executed in the event of an interruption of services. An effective DR plan is documented and designed to quickly and completely reestablish a system or service following a service interruption or disaster resulting in minimum loss to the organization. We performed audit work to determine the current status of DR planning throughout state government.

Since June 2009, the Legislative Audit Division has issued three separate Information Systems audit reports recommending agencies implement, maintain, and test DR plans. The agency responses to our recommendations ranged from acceptance of responsibility to recover its system and the need to do more planning, to belief that existing planning was adequate because they have contracted with ITSD to handle recovery. Given our identification of issues regarding DR planning and the variety of responses to our recommendations, we decided to perform audit work from a statewide perspective to determine what DR planning means to state agencies, and get a sense of the level of planning agencies have taken in recovering their information technology systems.

Background

Despite the term of disaster recovery, critical IT outages can occur under a number of scenarios that do not involve catastrophic events. While not as devastating, but more likely, IT outages can be the result of equipment failures, viruses, hackers, floods, theft, electrical outages, fires, and human errors. Figure 1 lists circumstances identified by 1,650 organizations worldwide that forced them to execute a DR plan.

Figure 1
Incidents Causing Initiation of DR Plans



Source: Compiled by the Legislative Audit Division from 2009 Symantec Disaster Recovery Survey.

Any system outage could limit or completely diminish the state's ability to provide services for the public or conduct basic administrative processes. The negative impacts of unpreparedness include extended downtime, unavailability of critical services, lost revenue, and loss of public trust. For these reasons, it is critical organizations limit downtime by implementing DR procedures.

There are a number of possible events which could force an organization to shut-down operations or lose connectivity, thus requiring the existence of a recovery plan. In recent years, Montana has experienced catastrophic wildfires. In September 2009, a wildfire ignited on McDonald Pass and moved to within six miles of the city. County officials informed Department of Administration officials they were prepared to evacuate the city of Helena if the fire progressed much further. Even without physical damage to

state buildings and equipment, the evacuation itself would have limited state agency access to their critical systems. The risk to each agency would depend on the extent of recovery planning in place, and how effective the plan is.

Within Montana State Government, many business processes are reliant on computer systems, with over $120 million in IT expenditures annually. Recently, the Information Technology Services Division at the Department of Administration has inventoried 427 computer systems in service throughout state government, each providing varied levels of support for agency business operations. If agencies are not developing DR plans to minimize system disruptions, the result could be extended unavailability of government services critical to the safety and welfare of the general public, as well as the day-to-day operations of state government. While we cannot put a specific dollar amount on damages, a study conducted by Symantec, a leading technology company, found organizations faced an average of $500,000 in losses per incident based on past outages. This study looked at 1,600 organizations worldwide, including financial, healthcare, and governmental entities.

Audit Objectives

DR planning represents an effective control to limit the negative impact on IT systems and to limit recovery costs resulting from a disaster or major outage. We developed the following audit objectives to determine if statewide DR planning is effective. Primarily, we wanted to establish if agencies have developed DR plans for the most critical systems, and if so, are those plans adequate. We consider an adequate DR plan as having elements suggested through established criteria and having tested and updated the completed plan. Our objectives were to:

1. Verify agencies have developed and documented DR plans for critical systems.
2. Determine if existing DR plans for critical systems meet established criteria.
3. Determine if agencies are testing DR plans.
4. Analyze results for agencies that have executed a DR plan.
5. Determine extent of centralized practices and tools in place affecting DR planning.

Audit Scope and Methodologies

During the planning of this audit, we issued a survey to all agency and university executives and elected officials to determine their views on DR planning and to measure the level of DR planning that has occurred at their respective entities. We found agencies are aware of the need for DR planning; however, there is a wide disparity in understanding and implementation of DR plans across agencies.

Through the results of our survey, we obtained a general idea of how DR planning is being implemented throughout the state. To achieve our objectives, we took additional steps to verify the existence of DR planning for critical systems. Given the number of systems within state government, it was not feasible to review DR plans for all systems. Rather, we identified systems considered critical and focused our audit work on those systems and the managing agencies.

We identified, through interview of agency personnel and review of survey results, the existence of DR plans. We also obtained available documentation and reviewed content to verify critical elements are included. We established criteria for the review by analyzing four separate sources, including federal guidelines and best practices, and developing a list of elements recommended by at least three of four sources. We also interviewed Department of Administration staff and reviewed laws and policies.

This audit was conducted in accordance with Government Auditing Standards published by the United States Government Accountability Office. We evaluated the control environment using generally applicable and accepted information technology standards.

Audit Overview

Based on our work, we conclude state agencies are aware of the need for DR planning for IT systems and most have incorporated some elements of a DR plan. However, we found the level of understanding of DR planning varies between agencies and some are more prepared to deal with extended system outages than others. We believe the inconsistency can be resolved by establishing centralized policy and corresponding guidelines requiring complete and consistent DR planning for IT systems.

Chapter II – Status of Disaster Recovery Planning

Introduction

To get a better sense of agency understanding and prioritization of Disaster Recovery (DR), as well as establish what DR is and what elements should be included based on established guidelines and practices, we established DR criteria, surveyed agency executives, and verified the existence and completeness of DR plans for critical agency systems.

Disaster Recovery Criteria

In order to establish criteria for disaster recovery procedures, we performed work to identify what is required of agencies in terms of DR planning. We found there are limited requirements detailing the development of DR Planning. The exception is the Montana Information Technology Act, which requires agencies to develop planning on how they intend to provide mission-critical services to Montana citizens and businesses (§2-17-524, MCA). In order to determine what constitutes DR planning, we looked to resources outside of statute or agency policy. These resources include federal standards, industry standards, industry best practices, and professionally recognized DR guidelines. The resources we used include:

- National Institute of Standards and Technology Contingency Planning Guidelines
- United States Agency for International Development Disaster Recovery Planning Procedures and Guidelines
- Information Technology (IT) Governance Institute Control Objectives for Information and Related Technology
- Continuity Central IT Disaster Recovery

To ensure we identified critical elements of DR planning, we selected elements that were identified by multiple sources. Eventually, we selected nine elements, which were included in at least three of our four sources. The criteria were then used to evaluate the level of DR planning at the agencies. The nine elements of a complete DR planning we identified are:

- Definition of roles and responsibilities of agency staff during and following a disaster or outage
- Detailed information of IT system recovery procedures to be implemented
- Procedures for testing the plan
- Expectations of time for recovery

- Identification and prioritization of critical services
- Usage guidelines (when the plan should be used)
- Communications guidelines (what information should be given to whom and how it should be shared)
- Location of a recovery site
- Inventory of equipment required for recovery

Disaster Recovery Survey

We developed and issued a survey to executives at 34 agencies and universities and received 26 responses. Our survey was intended to assist with identifying agency understanding and implementation of disaster recovery by:

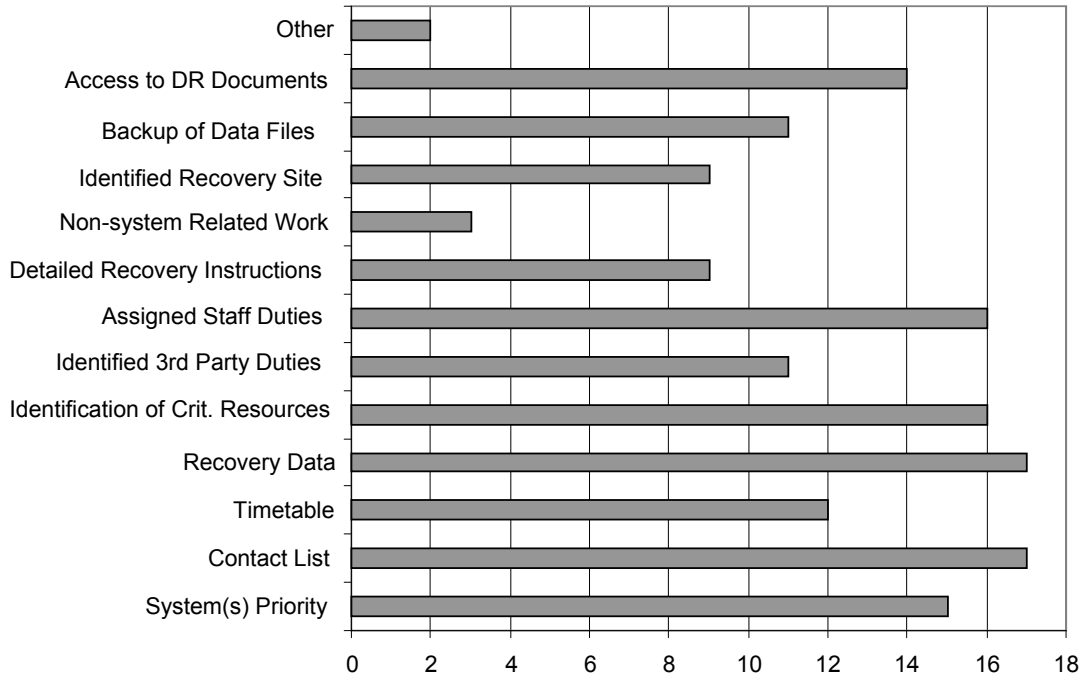
- Identifying agency definitions of DR
- Confirming the existence and documentation of DR plans
- Determining why agencies have not developed a DR plan(s)
- Identifying elements included in developed DR plans
- Determining if DR plans have been tested
- Determining if DR plans have been implemented at any point

The results of our survey showed a wide disparity among the respondents in understanding DR and the level to which DR plans have been implemented. The following list shows some of the key indications from the survey:

- 68 percent have developed DR procedures
- 57 percent have written a DR written plan
- 39 percent have tested DR plans
- Of the 8 responding agencies that do not have a DR plan, 7 have plans to develop one in the future
- Some of the reasons for not having a DR plan include reliance on Information Technology Services Division (ITSD), lack of resources, and cost

Our survey indicates 32 percent of agencies have not developed a plan for recovery, and 43 percent of agencies have not documented recovery plans, which we consider inadequate planning for these IT systems. Another concern was the variety of responses we received from agencies with DR plans regarding what elements they have integrated into procedures. Figure 2 shows different elements included in existing plans.

Figure 2
Elements Included in Existing DR Plans



Source: Compiled by the Legislative Audit Division.

Identifying Critical Systems

Because there are more than 400 systems throughout the state, it would not be feasible to review DR planning for all systems. We selected a sample based on the critical nature of each system.

Using documentation established by ITSD to identify essential functions within state government and our professional judgment, we identified IT systems critical to state business processes. We defined critical systems based on the following categories:

- Public Safety
- Revenue Generating
- Economic Impact
- Government Administration
- Health and Wellness
- Confidential Data
- Educational Services

Based on our analysis, we chose 12 systems at 11 different agencies to include in our audit work. Information on each of these systems can be found in Appendix A.

Agencies Aware of Need for Disaster Recovery

As part of our audit work, we met with agency representatives in regard to DR planning for each of the 12 systems. Through interviews with agency personnel and review of documentation, we noted each agency was aware of the risk and possible losses resulting from extended outages and understood the importance of having recovery procedures in place. While only six of the agencies we tested have developed a DR plan, all of the agencies we reviewed have implemented some elements of DR planning using other types of documentation. Elements were identified in DR planning documents, or in other agency produced documents including continuity of operations plans, business resumption plans, service level agreements, third-party contracts, and process flow-charts.

Conclusion

Agencies are aware of the need for DR planning, and have implemented elements of DR planning.

Obstacles to Agency Disaster Recovery Planning

Five of the eleven agencies we met with told us resources, including cost and staffing, were an obstacle to developing, implementing, and testing DR plans. Gartner, a major private firm in IT industry research, indicates the average IT-DR budget is $150,000. The majority of this amount is spent on annual tests of the DR plan.

DR Plan Testing

Testing of DR plans is the most effective way to make sure DR procedures are in place and to estimate the time of recovery without having the stress of a real disaster or outage. This is typically accomplished by shutting down the primary system, including supporting hardware and software, and then recovering a secondary system from an alternative location. Currently, most DR testing that occurs at state agencies is coordinated with ITSD. ITSD has a contract with a third-party to provide an alternate site for recovery. Included in the contract is 72 hours of testing time, which typically allows for one testing session a year. In addition, ITSD representatives state each testing session costs ITSD and the participating agencies an additional $20,000 per test session due to time spent for staff preparation and travel to the alternate site in Philadelphia.

This current testing environment only allows for four or five agencies to participate annually, and does carry a substantial cost to the state considering the cost of the contract and test preparation. In this sense, agencies are justified in concerns regarding cost, especially when there is no guarantee they will even have the opportunity to test given the limited number of hours offered by the vendor. However, there are upcoming changes to the state IT environment that should improve this situation.

There are currently plans underway by ITSD to develop two new datacenters. There will be a primary location in Helena, and a secondary location in Miles City. Since the state will operate and manage the new datacenters, the need for contract services will be reduced, resulting in lower cost. In addition, Miles City will act as the new alternate site and costs should be lowered by minimized preparation and travel time. Another benefit of the close proximity and lowered costs is more opportunities for agencies to test DR plans.

Available Staffing

Another cost some agencies indicate has mitigated DR efforts is the need for staff. Primarily, because DR planning is not a requirement, agency management has assigned DR responsibilities to staff. As a result, some agencies have not devoted enough resources to develop complete and effective DR plans. However, ITSD currently offers tools to ease the amount of time and effort needed to complete DR plans for critical systems.

The Department of Military Affairs purchased software called the Living Disaster Recovery Planning System (LDRPS) using a grant from the Department of Homeland Security. The LDRPS is managed and maintained by the Department of Administration. The software provides users with various templates for continuity of business processes and IT DR. During audit work, we reviewed the business continuity and IT DR templates offered through the LDRPS and concluded they have addressed all elements identified in our criteria, with the exception of the actual testing of the plan. Proper use of the LDRPS would involve the business process owners at each agency completing the Business Continuity template which includes recovery time objectives, location of recovery site, and identification and prioritization of IT systems. IT staff are then expected to complete the IT DR template including equipment inventory, recovery procedures, communication guidelines, and roles and responsibilities.

Disaster Recovery Is Expected Cost of IT Maintenance

DR planning is a critical component of a stable IT environment. Although there are costs associated with developing, maintaining, and testing a DR plan, that cost is

outweighed by the losses that could occur if critical systems are down for extended time and agencies are not prepared to recover. During our audit, we spoke with four agencies that have implemented elements of their DR plans due to a number of factors including IT failures, viruses, environmental issues, and routine maintenance. While none of the agencies have quantitative evidence of how DR planning benefited operations, they all agreed that having a plan was a benefit and mitigated the amount of downtime experienced. In contrast, we spoke with another agency that had experienced an outage due to a virus and had only a partial DR plan. They indicated the incomplete and untested plan caused additional problems and potentially worsened the problem. From that experience, they recognized the need for stronger DR planning and are currently updating their plan.

The cost of IT downtime can be significant considering the state's reliance on IT systems to provide public services, issue public safety warnings, generate revenue, administer government, etc. The cost of losing these services outweighs the expense of developing and maintaining a complete DR plan. In addition, ITSD has taken steps to lower future costs by establishing data centers with redundant capabilities, as well as offering an established method for creating an effective DR plan through use of the LDRPS.

CONCLUSION

Obstacles can impact DR planning, but ITSD is taking steps to mitigate obstacles.

Disaster Recovery Is a Shared Responsibility

Each agency is responsible for all applications it operates and manages. However, agencies will often sign a Service Level Agreement (SLA) with ITSD, where ITSD will house, operate, and maintain the servers where system files are stored. Also, SLAs typically address what ITSD will provide for recovery of a system. As part of our work, we reviewed SLAs between ITSD and the 11 agencies we reviewed to determine if all elements of our criteria are covered in the SLAs.

We found a number of the elements in established criteria are addressed in the SLAs we reviewed. Particularly, ITSD will provide some recovery procedures including backing-up data to an alternative site and restoring the application. While SLAs differ from agency to agency, some also include recovery time, equipment inventory, and requirements for agencies to be involved in the testing process. However, there are still elements that are not included in SLAs and must be completed by the agency including:

- Assignment of roles and responsibilities of staff during disaster or outage.
- Prioritization of the plan based on other systems and processes in the agency.
- Instructions on what conditions are to be met before a DR plan is implemented.
- Instructions on how information is to be communicated to key staff during a disaster or major outage.

In addition, while ITSD will perform key procedural steps in recovering a system, ITSD staff are not the system owners and cannot verify if a system is working as expected when the hardware is restored. This requires agencies to implement internal procedures to test and operate the system to ensure it is working and critical data has not been lost. We also asked each agency where the responsibility of DR falls and all but one of the eleven acknowledge that agencies share some level of responsibility for the recovery of systems.

CONCLUSION

Both agencies and ITSD have responsibilities for recovering systems.

Agency Implementation of DR Is Inconsistent

While we note all agencies have considered DR planning, and all have implemented some elements to restore critical systems, we also identified disparities in the level of completeness, and inconsistent implementation of DR plans. Based on our audit work, agencies have implemented anywhere from one to all nine of the elements of our criteria. In addition, there is no consistency on which DR elements should be included at a minimum. As represented in Figure 3, there is a significant variation on what elements of our criteria have been implemented from system to system.

Figure 3
Elements of DR Plans for Critical Systems

System	ID Roles	Recovery Procedures	Testing	Recovery Time	ID Critical	Usage Guide	Communication Guide	Recovery Site	Equipment Inventory	Totals
ALS	■	■	■		■	■	■			6
OMIS	■		■				■			3
MISTICS	■				■	■	■	■		5
CJIN	■	■	■		■	■	■	■	■	8
RWIS						■	■	■		3
IRIS	■			■	■					3
CEDARS				■			■	■		3
ClaimCenter	■	■	■	■	■	■	■	■	■	9
SVRS	■		■	■	■	■	■	■	■	8
SABHRS FS				■	■	■	■	■	■	6
SABHRS HR	■	■		■	■	■	■	■	■	8
AIM			■	■				■		3
Totals	**8**	**4**	**6**	**7**	**8**	**8**	**10**	**9**	**5**	

Source: Compiled by the Legislative Audit Division.

Four systems noted above (ClaimCenter, CJIN, SVRS, and SABHRS HR) have taken steps to recover from a serious outage because the managing agencies have implemented eight or nine of the elements identified in our criteria. While all the agencies have implemented some level of DR, we noted instances where critical elements were not addressed for many of the systems we reviewed. In addition, we identified a lack of consistency between agencies.

Agencies Need Guidance in Planning for Disaster

In the preliminary stages of this audit, we noted there are currently no requirements, state statutes, or established policies, requiring agencies to develop or implement DR procedures. As a result, there are no specific requirements as to what constitutes a complete and effective DR plan. Based on our discussion with agency representatives, additional guidance would assist them in developing more effective DR plans.

There are currently no requirements for agencies to develop DR plans. State statute establishes the Department of Military Affairs (DMA) as the agency responsible for emergency preparedness for the entire state of Montana (§10-3-101, MCA). Part of this responsibility is to develop an emergency preparedness plan. In this plan, DMA identifies the Department of Administration as the responsible party for all preparedness within state government. In addition, the Montana Information Technology Act tasks

the Department of Administration with establishing and enforcing policies related to information technology (§2-17-512, MCA).

Currently, the Information Technology Services Division provides support for agencies developing business continuity and DR procedures. In addition, ITSD has obtained software to assist in developing business continuity and DR documentation. However, ITSD has not established policies regarding DR planning. Considering our review of critical systems, state policy is needed to ensure agencies are developing complete and consistent procedures for recovering critical systems during a disaster or outage.

RECOMMENDATION #1

We recommend the Department of Administration develop policy including criteria for disaster recovery planning for State information technology systems.

Appendix A

Systems Selected for Review

Integrated Revenue Information System (IRIS) – Tax processing system managed by the Department of Revenue.

Automated Licensing System (ALS) – Managed by Fish, Wildlife and Parks to administer sporting license transactions.

Offender Management Information System (OMIS) – Used by the Department of Corrections to track movement of felony offenders.

Criminal Justice Information System (CJIN) – Managed by Department of Justice to provide information to law enforcement, including criminal background and motor vehicle records.

Road Weather Information System (RWIS) – Managed by Department of Transportation to provide travel conditions to the public.

Statewide Accounting, Budgeting, and Human Resources System (SABHRS) – Managed by the Department of Administration to assist agencies in administering financial accounts and human resources.

Montana Integrated System To Improve Customer Service (MISTICS) – Used by the Department of Labor and Industry to administer unemployment insurance.

Achievement in Montana (AIM) – Managed by the Office of Public Instruction to administer and report student records.

Consolidated Environmental Data Access and Retrieval System (CEDARS) – The Department of Environmental Quality maintains and operates this system to assist in the administration of environmental data, including permits and fines.

Statewide Voter Registration System (SVRS) – Implemented by the Secretary of State to administer voter records.

ClaimCenter – System maintained by Montana State Fund to assist in the administration of worker's compensation claims.

Department of Administration

Department Response

DEPARTMENT OF ADMINISTRATION
DIRECTOR'S OFFICE

B-1

BRIAN SCHWEITZER, GOVERNOR

JANET R. KELLY, DIRECTOR

STATE OF MONTANA

(406) 444-2032
FAX (406) 444-6194

MITCHELL BUILDING
125 N. ROBERTS, RM 155
PO BOX 200101
HELENA, MONTANA 59620-0101

February 5, 2010

Ms. Tori Hunthausen
Legislative Auditor
Legislative Audit Division
PO Box 201705
Helena, MT 59620-1705

RE: Information Systems Audit #10DP-01: Statewide Disaster Recovery Planning for Critical Information Technology Systems.

Dear Ms. Hunthausen:

The Department of Administration has reviewed the Information Systems Audit #10DP-01: Statewide Disaster Recovery Planning for Critical Information Technology Systems. Our response to the recommendation is below.

Recommendation #1

We recommend the Department of Administration develop policy including criteria for disaster recovery planning for State Information Technology Systems.

Response: Concur. The Department of Administration will develop policy including criteria for disaster recovery planning for State Information Technology Systems.

I want to thank you and your staff for their hard work and careful examination during this audit. We always look upon the audit process as an opportunity to improve the department's operations and performance.

The Department's Corrective Action Plan (CAP) is enclosed.

Sincerely,

Janet R. Kelly, Director

Enclosure

Preliminary Response
Corrective Action Plan (CAP): Audit Report #010DP-01
Statewide Disaster Recovery Planning for Critical Information Technology Systems
Department of Administration (DOA)
February 5, 2010

Agency	Recommendation #	Does this affect a federal program?	CFDA # (if previous YES)	Management View	CAP – Corrective Action Plan	Person responsible for CAP	Target Date
61010 DOA	**Recommendation #1** We recommend the Department of Administration develop policy including criteria for disaster recovery planning for State Information Technology System systems.	No		Concur	The Department of Administration will develop policy including criteria for disaster recovery planning for State Information Technology Systems.	Dawn Pizzini	July 1, 2011